Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 1997		**00-00-1997 to 00-00-1997**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Challenges in Computer Security Education	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Center for Information Systems Security Studies & Research (CISR),Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
IEEE Software, Vol. 14, No. 5, pp. 110-111, 1997

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**2**	

Challenges in Computer Security Education

Cynthia E. Irvine
Naval Postgraduate School Center for Infosec Studies and Research

A FRIEND OF MINE WAS PART OF A team assigned to build a networking product. Just as they were finishing up someone asked, "What about security?" At that point, it was a little late to do much about the system's security architecture, so they ultimately rolled out the product with a sprinkling of security sugar. The customer, who didn't even know how to ask for security, was pleased—and probably will be until disaster strikes.

At least some computer security instruction should be a prerequisite for participating in the Information Age.

This is just one example of the insufficient attention paid to security engineering and the secure use of computers. Companies are often unaware of even the most rudimentary procedures for securing their systems, while in the computer industry careful security engineering is left in the dust of rapid release cycles. Although awareness is increasing about the need for better computer security, to actually move in that direction we need people who know what they want, people who can build secure systems, and people who can manage those systems so they stay secure.

For three days last January, an international group met to discuss some of these issues at the First ACM Workshop on Education in Computer Security, held in Monterey, California. Representatives from 20 universities and a sprinkling of information systems security employers from industry and government were invited to attend based on position papers they had written. The group's task was to discuss ways to address the impending crisis in information security education. Among the questions addressed were articulating the diversity of information security education requirements for different careers and the need for training and retaining security experts in education.

WHOM TO EDUCATE? Although not the workshop's primary focus, some discussion centered on the need to instill notions of information responsibility in children from a very early age. This term encompasses not only computer use that ensures personal information security, but also includes a recognition of the social obligation to respect the security and privacy of other people's information. The consensus was that teaching information responsibility cannot be limited to one or two special classes; children must learn it by watching parents, teachers, and other adults act accordingly. As one attendee pointed out during a discussion period, children must learn to condemn rather than glorify hackers.

Attendees also agreed that at least some instruction in computer security should be a prerequisite for participating in the Information Age. Many educational institutions offer computer literacy courses for a broad spectrum of students. Although such courses cannot offer in-depth information security education, they can reinforce notions of information responsibility. Students can learn key security concepts and the dangers that can result from using computers carelessly. In addition, teachers can use various laboratory exercises to teach students how to keep their computers secure and use security support tools.

Participants realized rather quickly that a definitive, all-encompassing list of security concepts and facts was unlikely to emerge any time soon. They agreed that—beyond computer literacy courses—security education at the university level should focus on technical issues. Topics concerning computer law (as distinguished from security policies) and studies of computer ethics should be relegated to the Law and Philosophy departments respectively. The enormity of the challenge for information security education is made apparent by a partial list of those who need computer security education, as described in the box "Securing Educational Needs" on page 111.

Workshop participants outlined appropriate curricula for many occupations listed. However, because most undergraduate programs are already tightly packed, adding information security courses would be extremely difficult. Thus, attendees conceded that beyond survey courses—which can provide undergraduates greater technical depth than a computer literacy class, but still little specialization—most of the advanced computer security courses needed by information security professionals would be part of graduate programs.

WHO WILL TEACH? One of the most significant problems addressed at the workshop was the need for more computer security educators. At some schools, computer security courses are swamped, while others offer no instruction whatsoever, leaving students to fend for themselves. Should industry suddenly demand a large cadre of security professionals, institutions of higher learning will be hard pressed to offer the needed information security courses. Also, with the lure of higher salaries, security professionals will find industry more attractive than academia; professors with information security expertise will be hard to find. And the competition from industry is certainly there, as one industry participant made clear: he had job openings for security evaluators that were unfilled due to a lack of qualified applicants.

Another challenge to security educators is the burden of course preparation. It is not uncommon for a professor to take 10 hours or more to prepare a two-hour lecture for a computer security class. This is a consequence not only of the many areas affected by computer security, such as operating systems, database systems, networks, mobile computing,

SECURING EDUCATIONAL NEEDS

Participants at the ACM workshop outlined educational needs according to job title and roles.

♦ *The general population* doesn't care about the details of computer security; they just want to get the job done. However, anyone using a computer, child or adult, should understand the concept of information responsibility, the dangers of careless computer use, and fundamentals for secure computer use.

♦ *Corporate information professionals* must understand the importance of security, present the cost/benefit analysis to management, and get their companies to invest in systems security. Like insurance, good security is invisible and you often don't know you need it until too late. Corporate information officers must understand legal and policy issues associated with computer security as well as the technical feasibility of specific measures.

♦ *Computer professionals*, although not primarily responsible for computer security, should understand fundamental security concepts and how to securely manage computers so that they will recognize when a product needs security built in, when their organization has a security problem, and where they can go for help.

♦ *System administrators* should know how to configure and maintain a system securely, from installing virus scanners and security patches to managing passwords and reviewing audit trails and, in a growing number of facilities, the management of encryption keys. They must be aware of many aspects of practical security. Because system administration is such a huge job, an organization may need special operators delegated to carry out certain security-related tasks.

♦ *Computer security emergency response teams* are at the epicenter of many computer security crises. They are notified of incidents and develop solutions for security vulnerabilities; they test and disseminate patches to security flaws in operating systems, applications, and network protocols.

♦ *Secure software and hardware developers*, when developing new components, should know how to build security into products. They should know how hardware can support security objectives and how software can leverage hardware to produce secure systems.

♦ *System architects* must understand how different security mechanisms within the system work together; a flawed component can obviate all other protection features. They must understand overall requirements and must be able to design a system that meets a variety of obligations, including security.

♦ *System certifiers* assess the security claims made for systems, usually evaluating them against standards such as the "Orange Book" (*Dept. Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, National Computer Security Center, 1985).

♦ *Legal professionals and law enforcement* must develop good laws associated with secure computer use. This requires not only legal training, but an understanding of the technology to which the laws and regulations will apply. Little is currently available in the way of guidelines for law enforcement regarding the identification, apprehension, and prosecution of cyberspace criminals.

♦ *Security researchers* push the technological envelope. They must understand the interplay between security and other system properties such as fault tolerance and real-time constraints. They should have a deep understanding of computer science and the scientific foundations of computer security, and have significant specialized knowledge in their area of research.

web computing, and so on, but also of rapidly changing technology. To solve some of these problems, workshop participants agreed on the need to help each other by sharing resources, particularly with those trying to launch security education programs.

Many young professors also find that computer security is not considered "mainstream" research and that focusing on it may present roadblocks to a long academic career. This tends to deter graduate students from specializing in computer security, which adds to the existing problems. Industry investment in colleges and universities was one way attendees discussed for legitimizing computer security education.

WHAT CAN BE DONE? Several initiatives emerged to help remedy some of the problems facing both experienced and novice computer security educators. First, to share news and ideas, a list server has been started by Ed Felten of Princeton University. To participate, send a message to: majordomo@cs.princeton.edu with a subject line of subscribe compsec-education.

Also, a Web site is being constructed by Heather Hinton at Ryerson Polytechnic University, with assistance from Derek Simmel (CERT), Marie Wright (Western Conn. State University), and Deborah Frinke (University of Idaho). The site, at http://www.ee.ryerson.ca:8080/~hhinton/compsec/security.html, is to help educators find security courses and curricula.

Finally, more workshops on computer security education are planned. Participants said they benefited from this year's workshop, emerging with a much broader view of the "big picture" for computer security education and an appreciation of different approaches to making security an integral part of computer education. ◆

News continues on p. 114